Microsoft

Understanding Microsoft Entra ID Protection Risk Signals

Etan Basseri
Senior Product Manager
Identity Security

Agenda

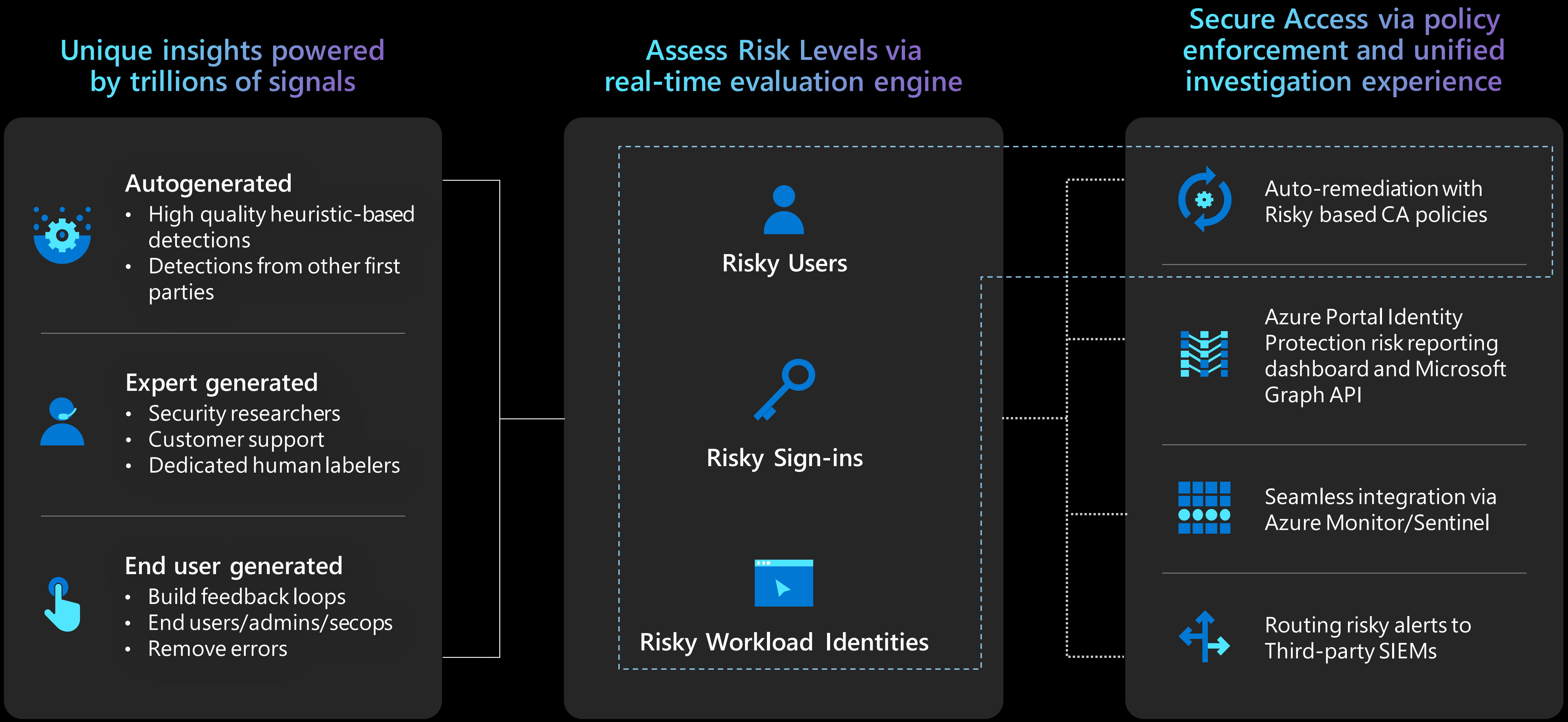
What is ID Protection?

How do the risk signals work?

Takeaways

What is ID Protection?

Entra ID Protection



Unique insights powered by trillions of signals

Autogenerated
- High quality heuristic-based detections
- Detections from other first parties

Expert generated
- Security researchers
- Customer support
- Dedicated human labelers

End user generated
- Build feedback loops
- End users/admins/secops
- Remove errors

Assess Risk Levels via real-time evaluation engine

Risky Users

Risky Sign-ins

Risky Workload Identities

Secure Access via policy enforcement and unified investigation experience

Auto-remediation with Risky based CA policies

Azure Portal Identity Protection risk reporting dashboard and Microsoft Graph API

Seamless integration via Azure Monitor/Sentinel

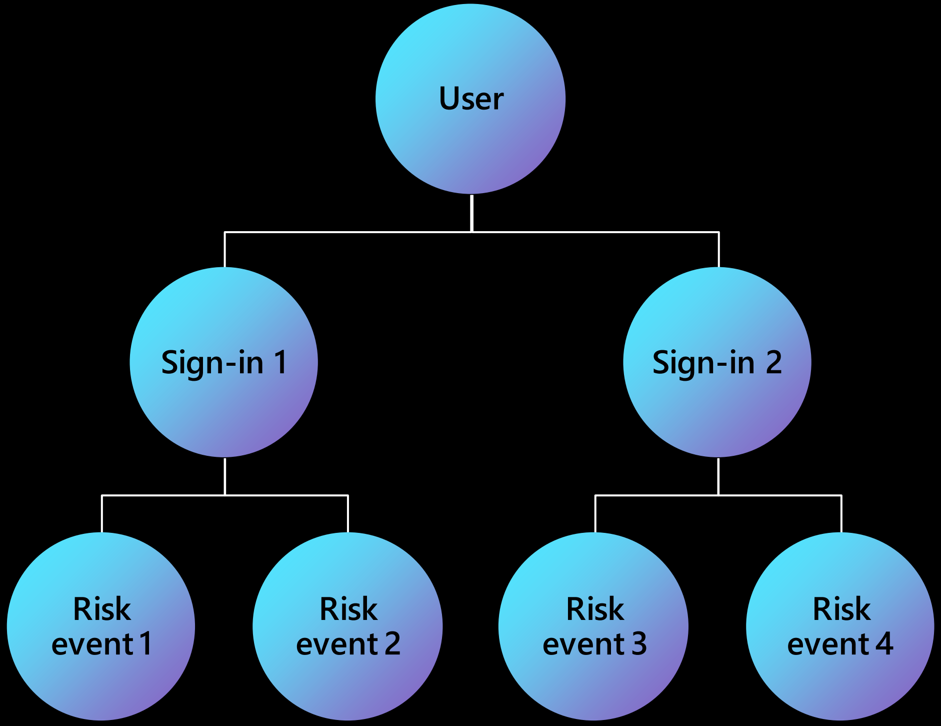
Routing risky alerts to Third-party SIEMs

Risky users, sign-in risk and detections

riskyUsers API
(read + write)

signIns API
(read + write*)

riskDetections API
(read only)

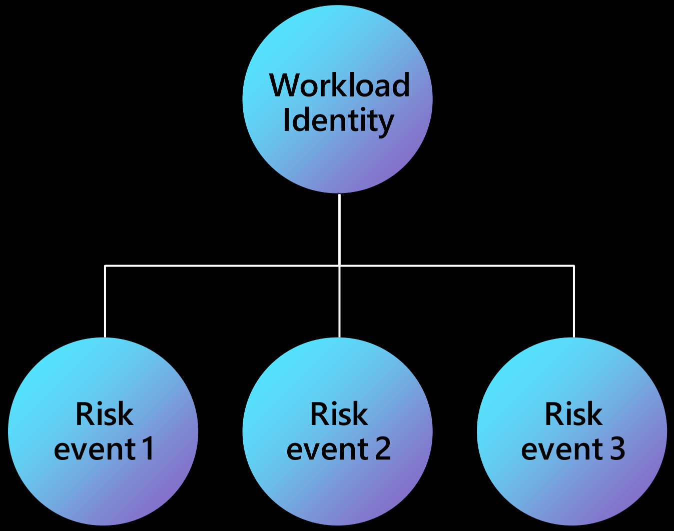


Risky workload identities and detections

Risk can come from SP behavior or something related to the app.

riskyServicePrincipals API
(read + write)

servicePrincipalRiskDetections API
(read only)



Choosing the right interface

1. APIs
2. Azure portal
3. Diagnostic settings
4. Microsoft Sentinel
5. Microsoft 365 Defender

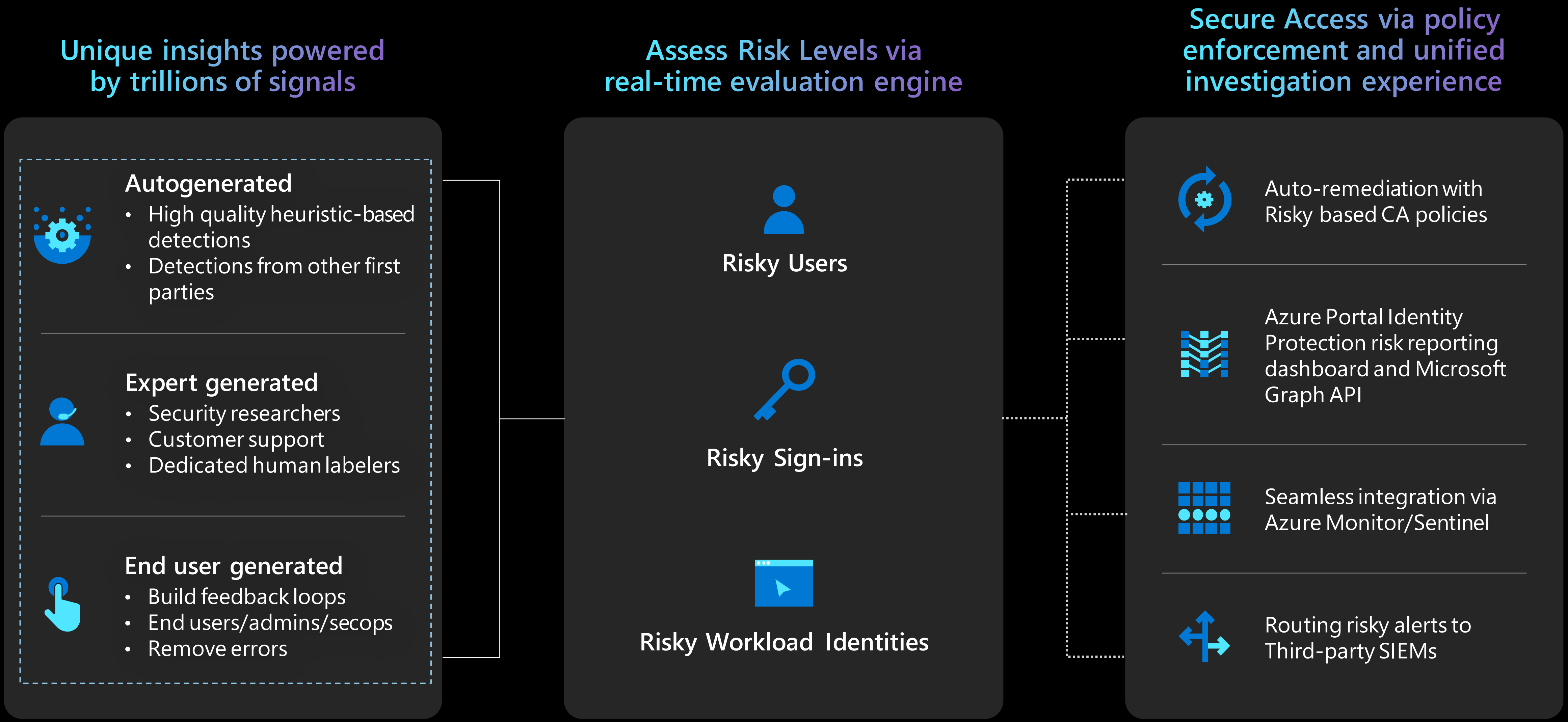
Risky sign-ins

```
GET /auditLogs/signIns?$filter=riskState eq 'atRisk'
```

```
{
  "id": "94f0b0aa-d195-4dcf-983d-e3122a130f00",
  "createdDateTime": "2022-04-13T23:30:11Z",
  "userDisplayName": "Jing Nghik",
  "userPrincipalName": "jinghik@woodgrove.ms",
  "userId": "360df853-0081-4b0d-af94-11dab1251fac",
  "appId": "38aa3b87-a06d-4817-b275-7a316988d93b",
  "appDisplayName": "Windows Sign In",
  "ipAddress": "20.106.98.167",
  "clientAppUsed": "Mobile Apps and Desktop clients",
  "correlationId": "e717be10-c87b-4966-a03d-6adf333e8d03",
  "conditionalAccessStatus": "notApplied",
  "isInteractive": true,
  "riskDetail": "none",
  "riskLevelAggregated": "low",
  "riskLevelDuringSignIn": "medium",
  "riskState": "atRisk",
  "riskEventTypes": [
    "unfamiliarFeatures"
  ],
  "riskEventTypes_v2": [
    "unfamiliarFeatures"
  ],
  "resourceDisplayName": "Windows Azure Active Directory",
  "resourceId": "00000002-0000-0000-c000-000000000000",
  "status": {
    "errorCode": 0,
    "failureReason": "Other.",
    "additionalDetails": null
  },
  ...
```

How do the risk signals work?

Entra ID Protection



Unique insights powered by trillions of signals

Autogenerated

- High quality heuristic-based detections
- Detections from other first parties

Expert generated

- Security researchers
- Customer support
- Dedicated human labelers

End user generated

- Build feedback loops
- End users/admins/secops
- Remove errors

Assess Risk Levels via real-time evaluation engine

Risky Users

Risky Sign-ins

Risky Workload Identities

Secure Access via policy enforcement and unified investigation experience

Auto-remediation with Risky based CA policies

Azure Portal Identity Protection risk reporting dashboard and Microsoft Graph API

Seamless integration via Azure Monitor/Sentinel

Routing risky alerts to Third-party SIEMs

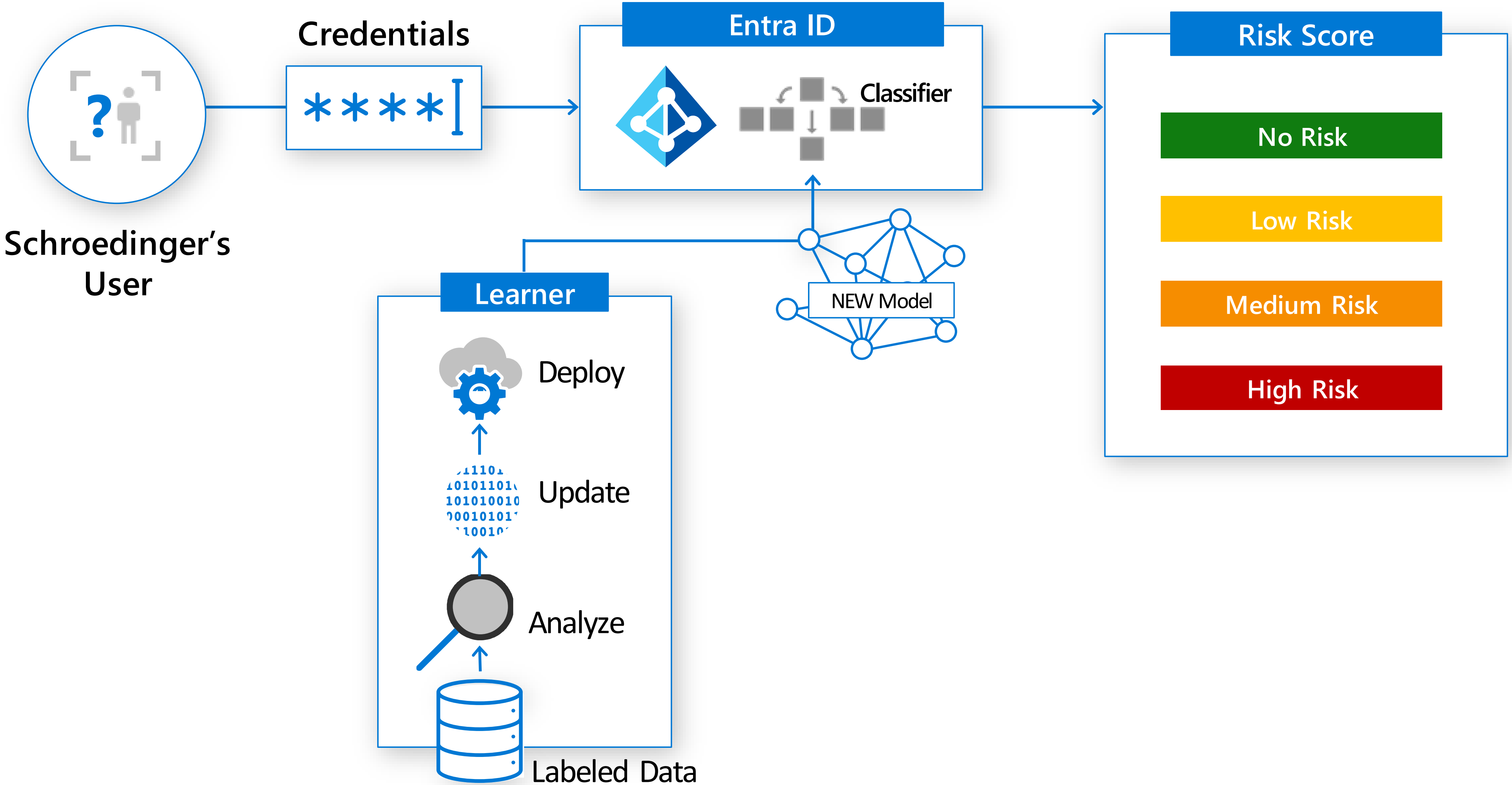
Signals

Autogenerated

Expert generated

End user generated

ML to calculate session risk

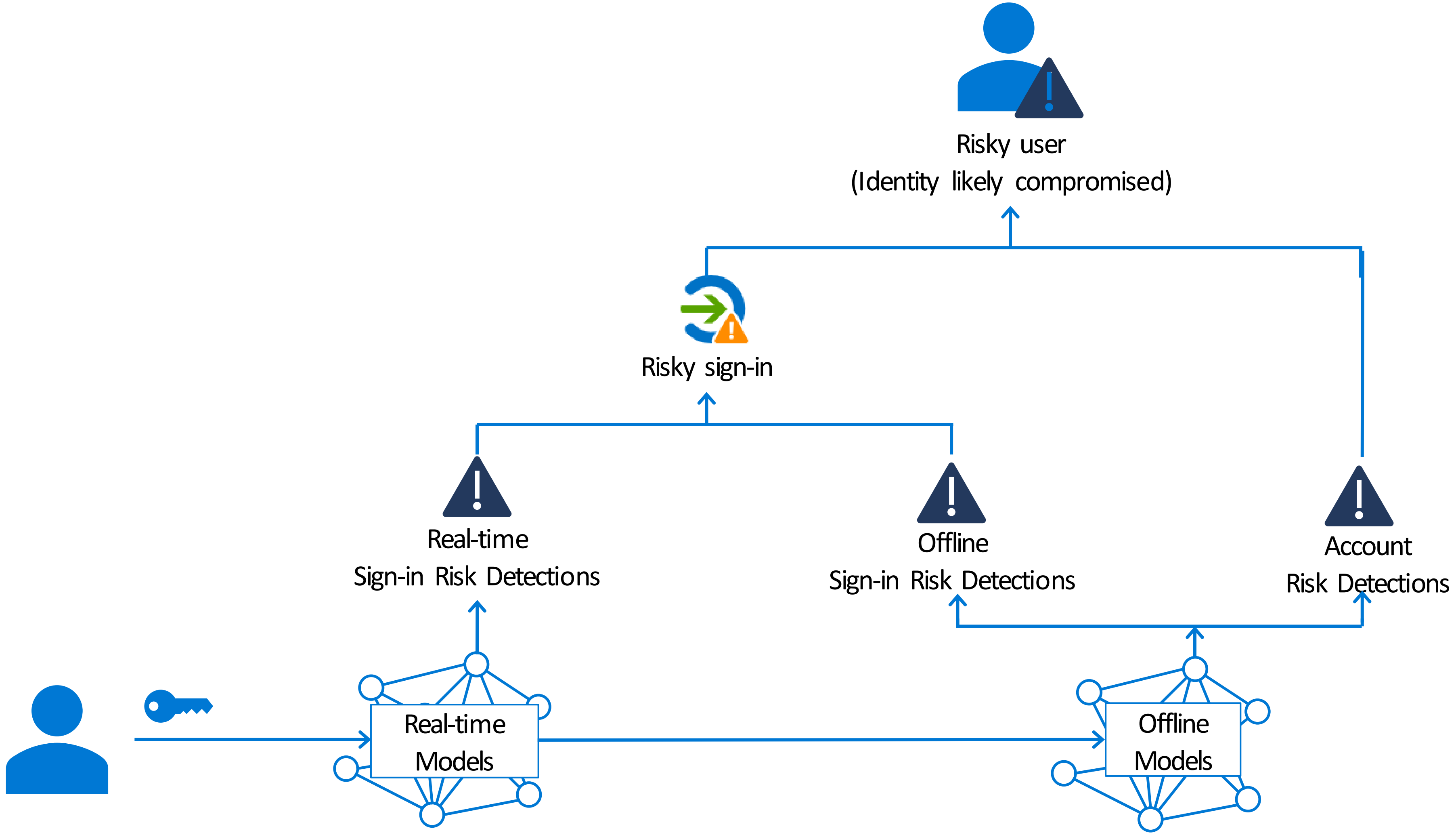


ML model weighting example

Feature	Model			
IsNormalTimeOfDay	lb			
IsFamiliarDevice	lb	lb	lb	
IsFamiliarApp	lb	lb		
IsFamiliarIP	lb	lb	lb	
IsFamiliarCountry	lb	lb	lb	lb
...				

- Model Training indicates what is the most important compromise indicators at that point in time based on the training data
- Allows the ML system adapt to new attacks on the fly, just retrain the model

Risk reporting



Risky user
(Identity likely compromised)

Risky sign-in

Real-time
Sign-in Risk Detections

Offline
Sign-in Risk Detections

Account
Risk Detections

Real-time
Models

Offline
Models

Other notable APIs

Conditional access

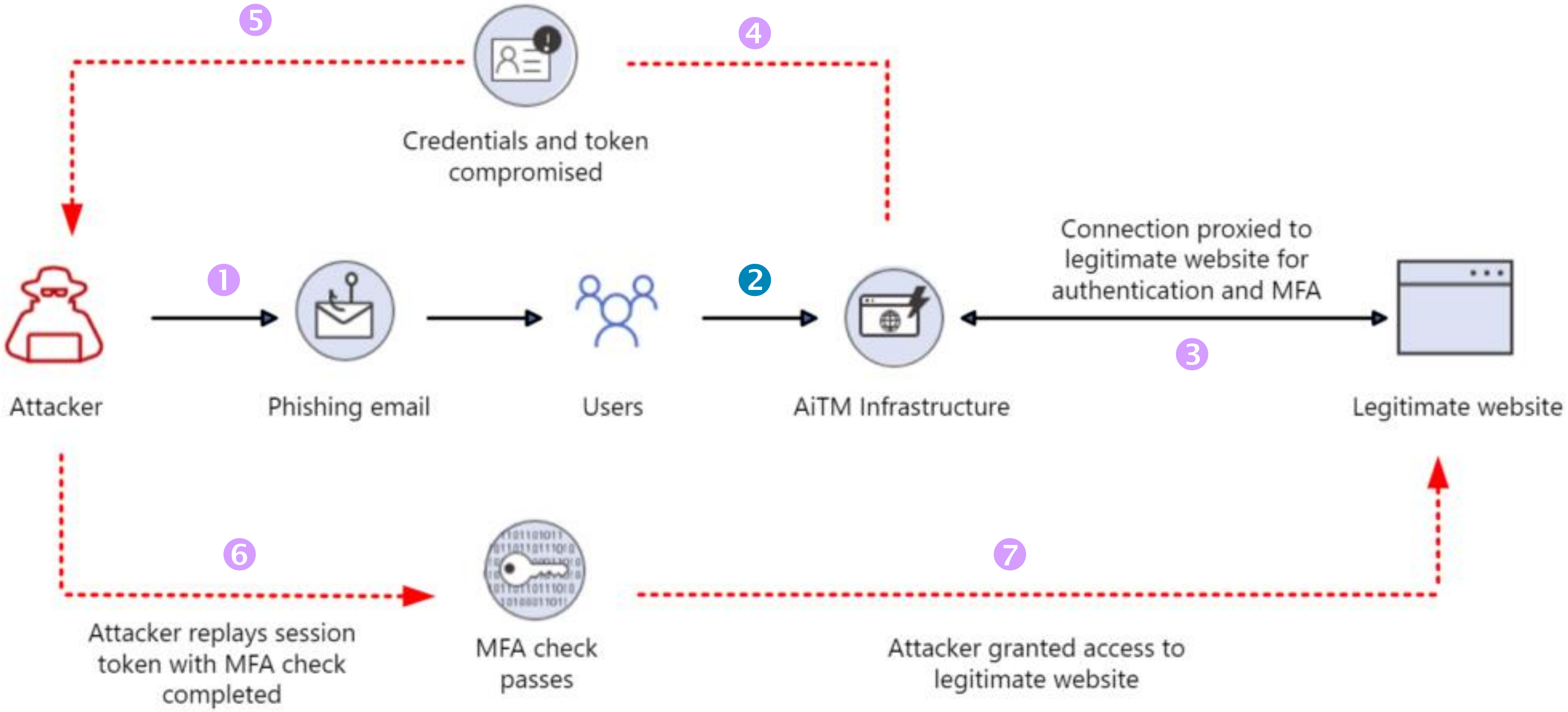
Named locations

Defining named locations and marking them as trusted can cut down on false positives for unfamiliar sign-in properties and atypical travel

Must be marked as trusted!!!

Token theft example

Adversary in the Middle


5
Credentials and token compromised
4
Attacker
1
Phishing email
Users
2
AiTM Infrastructure
Connection proxied to legitimate website for authentication and MFA
3
Legitimate website
6
Attacker replays session token with MFA check completed
MFA check passes
7
Attacker granted access to legitimate website

MITRE ATT&CK ID: T1557

Sign-in anomalies

Location

IP address

ASN

Country

Token lifetime

Unusually old tokens

Tokens played out of order

Device

Different Browser/OS

Client config

Auth failures

Missing required claims in token

Unexpected token for context

Resource

Should this identity + device + token type be accessing this resource?

Endpoint anomalies

Malware

Access to browser cookies

Access to on-device creds store

Phishing

Browser access to suspicious URLs

Remote access

Unexpected remote access

Access from unknown network

Post-auth behavior

Recon

Directory enumeration

Exfiltration

Mass access to email, files, cloud resources

Persistence

New device enrollment

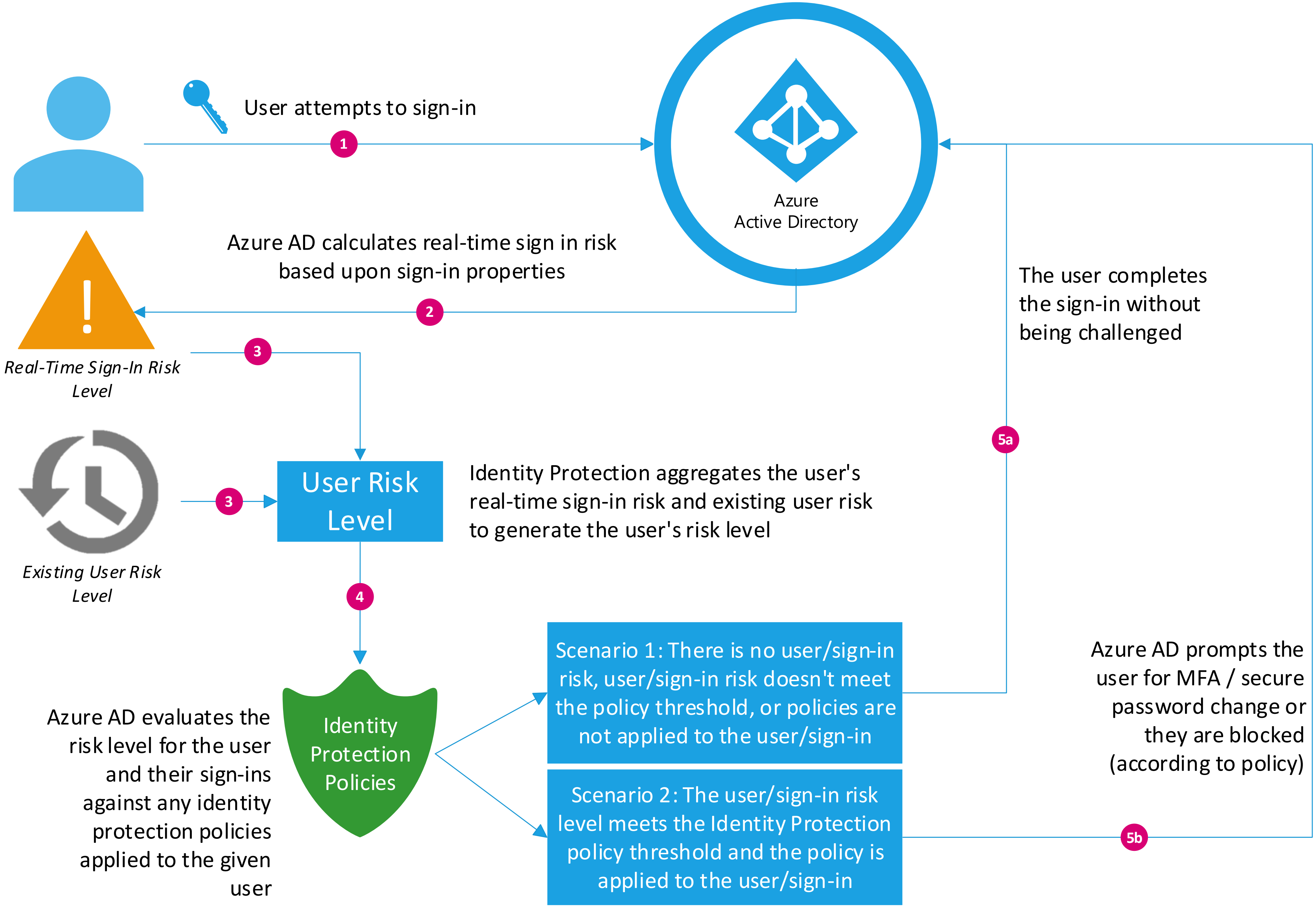
Creation of new accounts

Privilege Escalation

Assignment of admin roles

Rule-based models

- Anonymous browsing (incl. Tor)
- Atypical travel
- Leaked credentials



1 User attempts to sign-in

Azure
Active Directory

2 Azure AD calculates real-time sign in risk based upon sign-in properties

Real-Time Sign-In Risk Level

Existing User Risk Level

3 User Risk Level

Identity Protection aggregates the user's real-time sign-in risk and existing user risk to generate the user's risk level

4 Identity Protection Policies

Azure AD evaluates the risk level for the user and their sign-ins against any identity protection policies applied to the given user

Scenario 1: There is no user/sign-in risk, user/sign-in risk doesn't meet the policy threshold, or policies are not applied to the user/sign-in

5a The user completes the sign-in without being challenged

Scenario 2: The user/sign-in risk level meets the Identity Protection policy threshold and the policy is applied to the user/sign-in

5b Azure AD prompts the user for MFA / secure password change or they are blocked (according to policy)

Signals

Autogenerated

Expert generated

End user generated

Verified threat actor IP

Calculated in real-time. This risk detection type indicates sign-in activity that is consistent with known IP addresses associated with nation state actors or cyber crime groups, based on Microsoft Threat Intelligence Center (MSTIC).

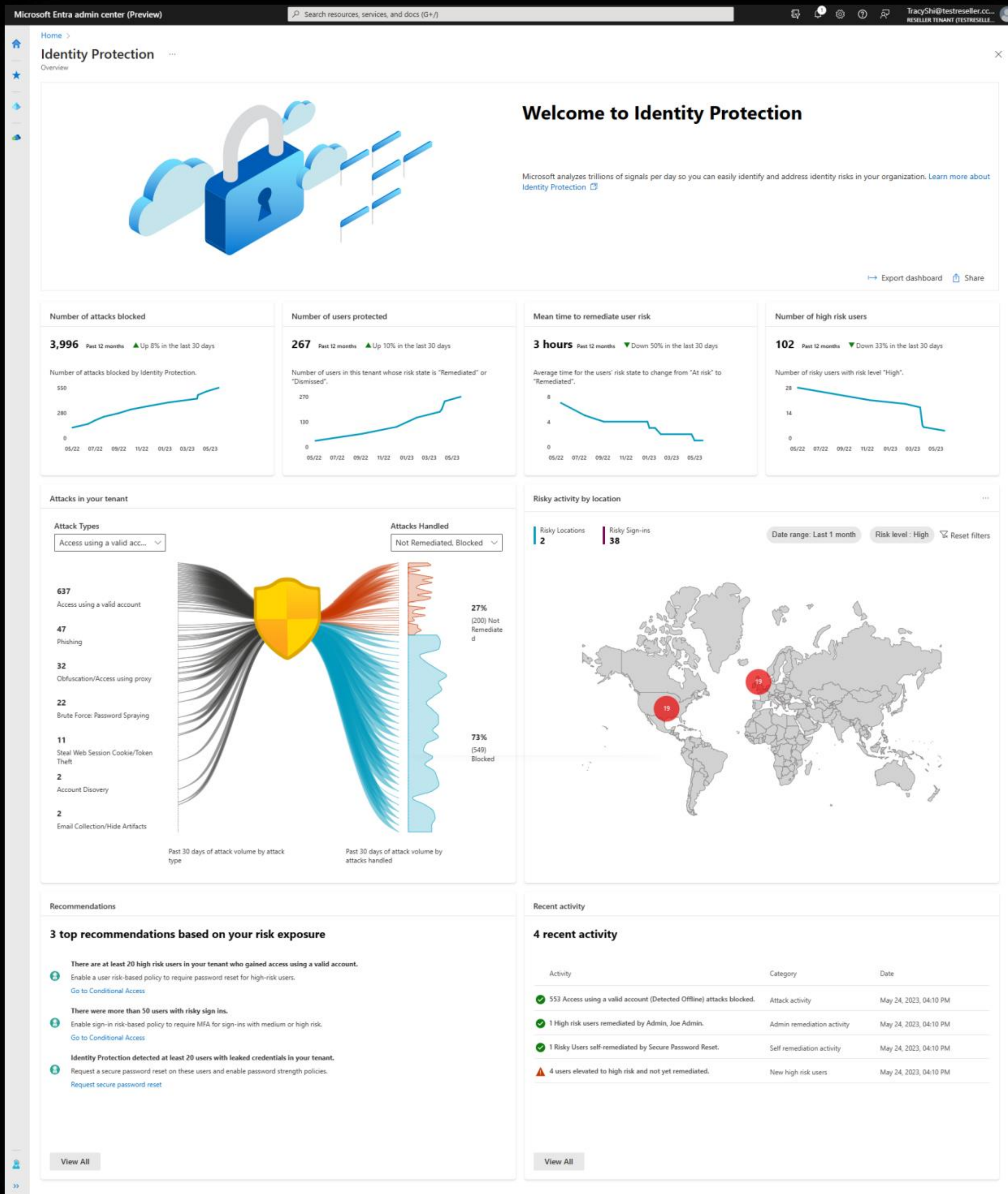
Signals

Autogenerated

Expert generated

End user generated

New landing page



Microsoft Entra admin center (Preview)
Search resources, services, and docs (G+/)
TracyShi@testreseller.cc...
RESELLER TENANT (TESTRESELLE...
Home

Identity Protection

Overview

Welcome to Identity Protection

Microsoft analyzes trillions of signals per day so you can easily identify and address identity risks in your organization. Learn more about Identity Protection

Number of attacks blocked

3,996 Past 12 months ▲Up 8% in the last 30 days

Number of attacks blocked by Identity Protection.

550
280
0
05/22
07/22
09/22
11/22
01/23
03/23
05/23

Number of users protected

267 Past 12 months ▲Up 10% in the last 30 days

Number of users in this tenant whose risk state is "Remediated" or "Dismissed".

Mean time to remediate user risk

3 hours Past 12 months ▼Down 50% in the last 30 days

Average time for the users' risk state to change from "At risk" to "Remediated".

Number of high risk users

102 Past 12 months ▼Down 33% in the last 30 days

Number of risky users with risk level "High".

Attacks in your tenant

Attack Types: Access using a valid acc...

Attacks Handled: Not Remediated, Blocked

637	Access using a valid account
47	Phishing
32	Obfuscation/Access using proxy
22	Brute Force: Password Spraying
11	Steal Web Session Cookie/Token Theft
2	Account Disovery
2	Email Collection/Hide Artifacts

27% (200) Not Remediate d

73% (549) Blocked

Past 30 days of attack volume by attack type

Past 30 days of attack volume by attacks handled

Risky activity by location

Risky Locations 2

Risky Sign-ins 38

Date range: Last 1 month

Risk level : High

Recommendations

3 top recommendations based on your risk exposure

There are at least 20 high risk users in your tenant who gained access using a valid account.
Enable a user risk-based policy to require password reset for high-risk users.
Go to Conditional Access

There were more than 50 users with risky sign ins.
Enable sign-in risk-based policy to require MFA for sign-ins with medium or high risk.
Go to Conditional Access

Identity Protection detected at least 20 users with leaked credentials in your tenant.
Request a secure password reset on these users and enable password strength policies.
Request secure password reset

Recent activity

4 recent activity

Activity	Category	Date
✓ 553 Access using a valid account (Detected Offline) attacks blocked.	Attack activity	May 24, 2023, 04:10 PM
✓ 1 High risk users remediated by Admin, Joe Admin.	Admin remediation activity	May 24, 2023, 04:10 PM
✓ 1 Risky Users self-remediated by Secure Password Reset.	Self remediation activity	May 24, 2023, 04:10 PM
⚠ 4 users elevated to high risk and not yet remediated.	New high risk users	May 24, 2023, 04:10 PM

Takeaways

Use Azure AD Conditional Access with risk-based policies

Use the APIs to get information and post operations to manage risk

Get Started

Documentation

aka.ms/securitysteps

aka.ms/IDPDeployment

aka.ms/AADIP-APIs

Sample Scripts

github.com/AzureAD/IdentityProtectionTools

Updates

docs.microsoft.com/en-us/azure/active-directory/fundamentals/whats-new